

**THE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF MISSOURI**

**IN THE MATTER OF THE SEARCH OF:
INFORMATION ASSOCIATED WITH
EMAIL ADDRESS "rosesman1982
@gmail.com," STORED AT THE
PREMISES CONTROLLED BY GOOGLE
LLC**

19-SW-02050-DPR

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Brian Martin, a Task Force Officer (TFO) with the Homeland Security Investigations, Immigration and Customs Office (HSI/ICE), being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with email address "rosesman1982@gmail.com," that is stored at premises owned, maintained, controlled, or operated by Google LLC ("PROVIDER"), an electronic communications services provider and/or remote computing services provider, which is headquartered at 1600 Amphitheatre Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require PROVIDER to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B, using the procedures described in Section III of Attachment B.

2. I have been employed as a Deputy Sheriff of Barry County, Missouri, since 1997 and a sworn law enforcement officer since 1985. As a TFO for HSI/ICE and a member of the Southwest Missouri Cyber Crimes Task Force (SMCCTF) in Joplin, Missouri, I have been assigned to investigate computer crimes, including violations against children. I have gained expertise in the conduct of such investigations through training in seminars, classes, and everyday work related to conducting these types of investigations. I have attended training provided by the Internet Crimes Against Children Program, the Federal Bureau of Investigation's Regional Computer Forensic Laboratory, and the Missouri Internet Crimes Against Children (ICAC) Task Force. I have written, executed, and assisted in over 200 search warrants on the state and federal level.

3. As part of my duties with ICE/HSI, I investigate criminal violations relating to child exploitation, child pornography, human trafficking, and coercion and enticement, in violation of 18 U.S.C. §§ 2251, 2252(a), 2252A, and 2422(a) and (b). I have received training in the areas of child pornography, child exploitation, and human/sex trafficking.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 2251, 2252(a), and 2252A(a); involving the use of a computer in or affecting interstate commerce to receive, possess, distribute, and produce child pornography, have been committed by Brian Turner using an account associated with the email address of "rosesman1982@gmail.com." There is also

probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

STATUTORY AUTHORITY

7. This investigation concerns alleged violations of Title 18, United States Code, Section 2251, 2252, and 2252A, relating to material involving the sexual exploitation of minors:

a. Title 18, United States Code, Section 2251(a) prohibits a person from employing, using, persuading, inducing, enticing, or coercing a minor to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce, or if such visual depiction actually was transported in or affecting interstate commerce.

b. Title 18, United States Code, Section 2252 prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce.

c. Title 18, United States Code, Section 2252A prohibits a person from

knowingly mailing, transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child pornography, as defined in 18 U.S.C. §2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

DEFINITIONS

8. The following definitions apply to this Affidavit and its Attachments:
 - a. The term “minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.
 - b. The term “sexually explicit conduct,” 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.
 - c. The term “visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.
 - d. The term “computer,” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in

conjunction with such device.

e. The term “child pornography,” as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

- i. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
- ii. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
- iii. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

f. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, and painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, and photocopies), mechanical form (including, but not limited to, phonograph records, printing, and typing) or electrical, electronic, or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or

electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

g. “Internet Service Providers” (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

h. “Internet Protocol address” (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet.

i. “Domain names” are common, easy to remember names associated with an IP address. For example, a domain name of “www.usdoj.gov” refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

j. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

PROBABLE CAUSE

9. On December 12, 2018, I received Cybertipline Report (CTR) 43046022 from the National Center for Missing and Exploited Children (NCMEC). It indicated that Facebook had discovered an image containing possible child pornography stored on their servers. Upon discovering the image, Facebook notified NCMEC on November 13, 2018.

10. Facebook reported that the user from the CTR had a profile name of “Brian Turner,” and a listed birth date of May 14, 1982. The file was sent by Facebook Messenger on November 11, 2018, from IP address 2600:0387:000b:0009:0000:0000:0000:00be, an AT&T Wireless IP address. On October 27, 2018, the account was logged into from IP address 2602:30a:2cda:2930:15e5:1eb5:b34a:8931, an AT&T Internet Services account.

11. I reviewed the file transmitted with the CTR, which had been previously viewed by Facebook. It is an image file that depicts a prepubescent female, no older than seven or eight, nude, standing against a wall with her leg raised high, exposing her vagina. Her breasts are also visible.

12. On January 29, 2018, I located Turner at a McDonald’s restaurant, located at 2115 East Independence Street, in Springfield, Missouri. In a post-*Miranda* interview, Turner admitted to viewing child pornography since he was 25. He explained that he received the child pornography from others utilizing Facebook Messenger. Turner also admitted that he stored images of child pornography in his Google Photos account that is associated with his email address of rosesman1982@gmail.com.

BACKGROUND CONCERNING PROVIDER’S ACCOUNTS

13. PROVIDER is the provider of the Internet-based account associated with the email address of rosesman1982@gmail.com.

14. PROVIDER provides its subscribers Internet-based accounts that allow them to send, receive, and store e-mails online.

15. Based on my training and experience, I know that PROVIDER allows subscribers to obtain accounts by registering on PROVIDER's website. During the registration process, PROVIDER asks subscribers to create a username and password, and to provide basic personal information such as a name, an alternate e-mail address for backup purposes, a phone number, and in some cases a means of payment. PROVIDER typically does not verify subscriber names. However, PROVIDER does verify the e-mail address or phone number provided.

16. Once a subscriber has registered an account, PROVIDER provides e-mail services that typically include folders such as an "inbox" and a "sent mail" folder, as well as electronic address books or contact lists, and all of those folders are linked to the subscriber's username. PROVIDER subscribers can also use that same username or account in connection with other services provided by PROVIDER. Here, PROVIDER's other services include: electronic communication services such as Google Voice (voice calls, voicemail, and SMS text messaging), Hangouts (instant messaging and video chats), Google+ (social networking), Google Groups (group discussions), Google Photos (photo sharing), and YouTube (video sharing); web browsing and search tools such as Google Search (Internet searches), Web History (bookmarks and recorded browsing history), and Google Chrome (web browser); online productivity tools such as Google Calendar, Google Contacts, Google Docs (word processing), Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and local business search) and other location services, and Language Tools (text translation); online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google AdWords (user targeting based on search queries); Pixel Phone (services which support a Google smartphone);

and Google Play (which allow users to purchase and download digital content, e.g., applications).

17. In general, user-generated content (such as e-mail) that is written using, stored on, sent from, or sent to a PROVIDER account can be permanently stored in connection with that account, unless the subscriber deletes the material. For example, if the subscriber does not delete an e-mail, the e-mail can remain on PROVIDER's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to exist on PROVIDER's servers for a certain period of time.

18. Thus, a subscriber's PROVIDER account can be used not only for e-mail but also for other types of electronic communication, including: instant messaging and photo and video sharing; voice calls, video chats, SMS text messaging; social networking. Depending on user settings, user-generated content derived from many of these services is normally stored on PROVIDER's servers until deleted by the subscriber. Similar to e-mails, such user-generated content can remain on PROVIDER's servers indefinitely if not deleted by the subscriber, and even after being deleted, it may continue to be available on PROVIDER's servers for a certain period of time. Furthermore, a PROVIDER subscriber can store: contacts, calendar data, images, videos, notes, documents, bookmarks, web searches, browsing history, and various other types of information on PROVIDER's servers. Based on my training and experience, I know that evidence of who controlled, used, and/or created a PROVIDER account may be found within such computer files and other information created or stored by the PROVIDER subscriber. Based on my training and experience, I know that the types of data discussed above can include records and communications that constitute evidence of criminal activity.

19. Based on my training and experience, I know that providers such as PROVIDER also collect and maintain information about their subscribers, including information about their use of PROVIDER services. This information can include the date on which the account was

created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. Providers such as PROVIDER also commonly have records of the IP address used to register the account and the IP addresses associated with other logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which devices were used to access the relevant account. Also, providers such as PROVIDER typically collect and maintain location data related to subscriber's use of PROVIDER services, including data derived from IP addresses and/or Global Positioning System ("GPS") data.

20. Based on my training and experience, I know that providers such as PROVIDER also collect information relating to the devices used to access a subscriber's account – such as laptop or desktop computers, cell phones, and tablet computers. Such devices can be identified in various ways. For example, some identifiers are assigned to a device by the manufacturer and relate to the specific machine or "hardware," some identifiers are assigned by a telephone carrier concerning a particular user account for cellular data or voice services, and some identifiers are actually assigned by PROVIDER in order to track what devices are using PROVIDER's accounts and services. Examples of these identifiers include unique application number, hardware model, operating system version, Global Unique Identifier ("GUID"), device serial number, mobile network information, telephone number, Media Access Control ("MAC") address, and International Mobile Equipment Identity ("IMEI"). Based on my training and experience, I know that such identifiers may constitute evidence of the crimes under investigation because they can be used (a) to find other PROVIDER accounts created or accessed by the same device and likely

belonging to the same user, (b) to find other types of accounts linked to the same device and user, and (c) to determine whether a particular device recovered during course of the investigation was used to access the PROVIDER account.

21. Based on my training and experience, I know that providers such as PROVIDER use cookies and similar technologies to track users visiting PROVIDER's webpages and using its products and services. Basically, a "cookie" is a small file containing a string of characters that a website attempts to place onto a user's computer. When that computer visits again, the website will recognize the cookie and thereby identify the same user who visited before. This sort of technology can be used to track users across multiple websites and online services belonging to PROVIDER. More sophisticated cookie technology can be used to identify users across devices and web browsers. From training and experience, I know that cookies and similar technology used by providers such as PROVIDER may constitute evidence of the criminal activity under investigation. By linking various accounts, devices, and online activity to the same user or users, cookies and linked information can help identify who was using a PROVIDER account and determine the scope of criminal activity.

22. Based on my training and experience, I know that PROVIDER maintains records that can link different PROVIDER accounts to one another, by virtue of common identifiers, such as common e-mail addresses, common telephone numbers, common device identifiers, common computer cookies, and common names or addresses, that can show a single person, or single group of persons, used multiple PROVIDER accounts. Based on my training and experience, I also know that evidence concerning the identity of such linked accounts can be useful evidence in identifying the person or persons who have used a particular PROVIDER account.

23. Based on my training and experience, I know that subscribers can communicate

directly with PROVIDER about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers such as PROVIDER typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

24. In summary, based on my training and experience in this context, I believe that the computers of PROVIDER are likely to contain user-generated content such as stored electronic communications (including retrieved and unretrieved e-mail for PROVIDER subscribers), as well as PROVIDER-generated information about its subscribers and their use of PROVIDER services and other online services. In my training and experience, all of that information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. In fact, even if subscribers provide PROVIDER with false information about their identities, that false information often nevertheless provides clues to their identities, locations, or illicit activities.

25. As explained above, information stored in connection with a PROVIDER account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element of the offense, or, alternatively, to exclude the innocent from further suspicion. From my training and experience, I know that the information stored in connection with a PROVIDER account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For

example, e-mail communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by PROVIDER can show how and when the account was accessed or used. For example, providers such as PROVIDER typically log the IP addresses from which users access the account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the PROVIDER account access and use relating to the criminal activity under investigation. This geographic and timeline information may tend to either inculcate or exculpate the person who controlled, used, and/or created the account. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via e-mail). Finally, stored electronic data may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information in the PROVIDER account may indicate its user's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

19. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on PROVIDER, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at

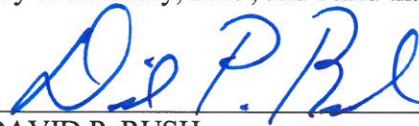
any time in the day or night. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Further Affiant Sayeth Not.



BRIAN E. MARTIN
Task Force Officer
Homeland Security Investigations

Sworn to and subscribed to me this 21st day of ~~February~~ ^{March}, 2019, and I find that probable cause exists.



DAVID P. RUSH
United States Magistrate Judge
Western District of Missouri